REMARKS

This Application has been carefully reviewed in light of the Office Action mailed April 9, 2004 ("Office Action"). At the time of the Office Action, Claims 1-36 were pending in the application. In the Office Action, the Examiner rejects Claims 1-36. In order to advance prosecution of this case, Applicant amends Claims 1, 6, 14, 28, and 33 and cancels Claim 25 without prejudice or disclaimer. Applicant respectfully requests reconsideration and favorable action in this case.

Claim Objections

The Examiner objects to Claims 23 and 25 because they are the exact same limitation and both are dependents of Claim 22. Applicant has canceled Claim 25. Accordingly, Applicant respectfully requests that the objection to Claim 23 be withdrawn.

Section 101 Rejections

The Examiner rejects Claims 1-34 under 35 U.S.C. § 101 because the language of the independent Claims 1, 6, 14, 28, and 33 raise a question as to whether the claims are directed merely to an abstract idea that is not tied to a technological art, environment, or machine which would result in a practical application. Specifically, the Examiner states that there is "nothing in any of the independent claims that would tie the algorithm to a particularly physical device such as a computer." (Office Action, page 2). Although Applicant believes that all previously pending claims recite statutory subject matter under § 101, to advance this case expeditiously to issuance, Applicant has amended independent Claims 1, 6, 14, 28, and 33 to address the issues identified by the Examiner. For at least these reasons, Applicant respectfully requests that the rejection of the Claims 1-40 under § 101 be withdrawn and the claims allowed.

Section 112 Rejections

The Examiner rejects Claim 6 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention. Applicant has amended Claim 6 to correct the typographical error identified by the Examiner. Accordingly, Applicant respectfully submits that Claim 6, as amended, is in accordance with § 112, second paragraph. Applicant requests that the rejection of Claim 6 be withdrawn.

Section 103 Rejections

The Examiner rejects Claims 1-36 under 35 U.S.C. § 103(a) as being unpatentable over "Secure Communications Over Insecure Channels," by Merkle ("*Merkle*") in view of U.S. Patent No. 5,815,573 issued to Johnson et al. ("*Johnson*"). For the following reasons, Applicant respectfully traverses these rejections.

First, Applicant respectfully submits that the proposed *Merkle-Johnson* combination does not disclose each and every feature as recited in Applicant's claims. Independent Claim 1, of the present Application, recites:

> A method for storing and withdrawing a decryption key from a key escrow database, comprising:
> creating, at a computer, a set of N trap door encryption-decryption function pairs each paired with a corresponding token;
> transmitting the set of N trap door encryption-decryption function pairs along with a corresponding token to a receiver, the transmission sent over a communication path coupling the receiver and the computer;
> randomly selecting at the receiver one of the trap door encryption-decryption function pairs and the corresponding token;
> adding randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair;
> encrypting the token with the added randomization information at the receiver, the token corresponding with the randomly selected encryption-decryption function pair;
> recording in a key escrow database the created set of N trap door encryption-decryption function pairs and the corresponding paired token;
> recording in the key escrow database the randomly selected trap door encryption-decryption function pair along with the encrypted token; and
> inverting the created set of N trap door encryption-decryption function pairs and the randomly selected trap door encryption-decryption function pair along with the encrypted token to identify the decryption key.

As one example, Applicant respectfully submits that the proposed *Merkle-Johnson* combination does not disclose, teach, or suggest "randomly selecting at the receiver one of the trap door encryption-decryption function pairs and the corresponding token . . . [and] adding randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair," as recited in Claim 1. The Examiner acknowledges that *Merkle* does not disclose the recited features and instead relies on *Johnson*. Applicant respectfully submits, however, that *Johnson* does not make up for the acknowledged deficiencies of *Merkle*. Although *Johnson* discloses a system for generating an encryption key for a pair of users (designated as Alice and Bob), *Johnson* discloses that Alice's system, as the originator, "begins by generating a 336-bit secret starting PQR (SPQR) value 202 (FIG. 2A)(step 502)." (Column 8, lines 64-66). "The SPQR value 202 is used by both Alice and Bob to generate a key K (118) . . . . used to encrypt and decrypt messages." (Column 8, line 67 through Column 9, line 2). With regard to key K(118), *Johnson* further discloses that "Alice's system creates a session header 312 (FIG. 3B-3C) containing protocol information, generates a cryptographic key (K) (118) from information stored in the session header, and encrypts a first message (message 1) with the key K to generate an encrypted message 1 (FIG. 3C)." Thus, Alice, as the originator, creates the key, which may be used by both Bob and Alice to decrypt messages. 8, lines 47-51).

After the key is generated, "Alice encrypts the SPQR value 202 with a public key of Bob's that is specifically intended for key distribution to generate an encrypted SPQR value SPQR' (step 504)." (Column 9, lines 7-9). The portions of the Specification relied on by the Examiner for the disclosure of the steps of adding randomized information and encrypting the token with the added randomized information merely discloses the inputs required for the generation of SPQR' by Alice. (Column 9, lines 1-61). *Johnson* then discloses that "[f]ollowing the encryption steps 504 and 506, Alice generates a session context block 302 containing the encrypted value SPQR' (304) . . . [and] digitally signs the session context 302 with her private signature key." (Column 10, line 57 through Column 11, line 2). "Finally, a packet 316 containing the session header 312 and the encrypted message 1 (314) are sent to Bob (step 518)." (Column 11, lines 3-5). Upon receiving the packet 316 from Alice, Bob's system merely "validates the signature 310 on the session context 302, using Alice's public

signature key" and "decrypts the encrypted SPQR value 304 (FIG. 3A) using his private decryption key to obtain the original SPQR value 202." (Column 11, lines 6-12). "Bob then regenerates the key 118 (FIG. 1) from the decrypted SPQR value 202 (FIG. 2A) using the procedure employed by Alice previously (step 608)." (Column 11, lines 20-22). Thus, Bob's system, as the recipient, merely decrypts the encoded message. To the extent that any randomizing information is added (which Applicant disputes), such a step is performed by Alice rather than Bob. As such, Applicant respectfully submits that the proposed *Merkle-Johnson* combination does not disclose, teach, or suggest "randomly selecting *at the receiver* one of the trap door encryption-decryption function pairs and the corresponding token . . . [and] adding randomization information *at the receiver* to the corresponding token of the selected trap door encryption-decryption function pair," as recited in Claim 1.

Second, assuming for purposes or argument that the proposed combination discloses the limitations of Applicant's claims, which Applicant disputes, it would not have been obvious to one skilled in the art to make the combination. The mere fact that references <u>can</u> be combined does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680 (Fed. Cir. 1990). The showing must be clear and particular. *See, e.g., C.R. Bard v. M3 Sys., Inc.*, 48 USPQ.2d 1225, 1232 (Fed. Cir. 1998). The Examiner has not provided adequate evidence of the required motivation or suggestion to make the proposed combination. The Examiner merely speculates "it would have been obvious" to make the proposed combination to "prevent the token from being sent in the clear over an unsecure channel." (Office Action, page 4). The Examiner has not shown any motivation to combine and instead simply relies upon hindsight. It is improper for an Examiner to use hindsight having read the Applicant's disclosure to arrive at an obviousness rejection. *In re* Fine, 837 F.2d 1071, 1075, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988). It is improper to use the claimed invention as an instruction manual or template to piece together the teachings of the prior art so that the claimed invention is rendered obvious. *In re* Fritch, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Because the Examiner has merely used Applicant's claims as an instruction manual to piece together the encryption system of *Merkle* with the method for key generation disclosed in *Johnson*, Applicant respectfully submits that the proposed *Merkle-Johnson* combination is improper and should not be used here to reject Applicant's claims.

For at least these reasons, Applicant respectfully requests reconsideration and allowance of Claim 1.

The Examiner also relies on the *Merkle-Johnson* combination to reject independent Claims 6, 14, 28, and 33. Applicant respectfully submits that the proposed *Merkle-Johnson* combination does not disclose, teach, or suggest each and every element of Applicant's independent claims. For example, Claim 6 recites "randomly selecting at the receiver one of the cryptogram/decryption key pairs along with the corresponding token" and "decrypting the randomly selected cryptogram utilizing the corresponding token to obtain a corresponding decryption key." Claims 14, 28 and 33 include certain similar, though not identical, features and operations. Thus, for reasons similar to those discussed above with regard to Claim 1, Applicant respectfully submits that neither *Merkle* nor *Johnson* disclose, teach, or suggest each and every element as set forth in Applicant's independent Claims 6, 14, 28, and 33.

Dependent Claims 2-5, 7-13, 15-27, 29-32, and 34-36 depend from independent Claims 1, 6, 14, 28, and 33, respectively, which Applicant has shown above to be allowable. Accordingly, dependent Claims 2-5, 7-13, 15-27, 29-32, and 34-36 are not obvious over the *Merkle-Johnson* combination at least because they include the limitations of their respective independent claims. Additionally, dependent Claims 2-5, 7-13, 15-27, 29-32, and 34-36 recite elements that further distinguish the art. As just one example, Claim 3 recites "randomly selecting at the receiver an additional trap door encryption-decryption function pair and the corresponding token" and "adding randomization information to the corresponding token of the additional selected trap door encryption-decryption function pair." Claims 7, 20, 22, 30, 34, and 36 recite certain similar, though not identical, features and operations. The Examiner acknowledges that *Merkle* does not explicitly teach the receiver selecting more than one of the puzzles to decrypt. (Office Action, page 10). The Examiner posits, however, that "one of ordinary skill in the art would know that the work needed to be performed by an eavesdropper plotting to learn the decryption key is $O(n^2)$" and that "the limitations of claim 3 are merely repeating an already disclosed limitation that does not produce an unobvious result." (Office Action, pages 10-11). For reasons similar to those discussed above with regard to Claim 1, Applicant respectfully submits that neither *Merkle*

nor *Johnson* discloses, teaches, or suggests the features and operations recited in dependent Claims 2-5, 7-13, 15-27, 29-32, and 34-36. To the extent that *Johnson* discloses adding randomizing information (which Applicant disputes), such a step is performed by the originator rather than by the receiver. For at least these reasons, Applicant respectfully requests reconsideration and allowance of Claims 2-5, 7-13, 15-27, 29-32, and 34-36.

CONCLUSION

Applicant has made an earnest attempt to place this case in condition for immediate allowance. For the foregoing reasons and for other reasons clear and apparent, Applicant respectfully requests reconsideration and allowance of the pending claims.

Applicant believes no fees are due. However, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

If there are matters that can be discussed by telephone to advance prosecution of this application, Applicant invites the Examiner to contact its attorney at the number provided below.

Respectfully submitted,

Baker Botts L.L.P.
Attorneys for Applicant

Kevin J. Meek
Reg. No. 33,738

Dated: July 1, 2004

CORRESPONDENCE ADDRESS:
2001 Ross Avenue, Suite 600
Dallas, Texas 75201-2980
(214) 953-6680

at Customer No.   05073